

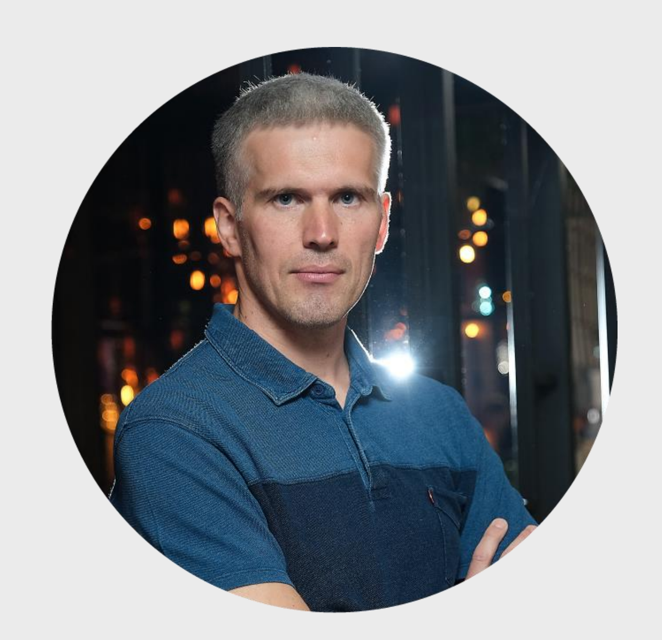
Как разобрать сетевой протокол и найти уязвимости в устройстве без использования прошивки, показываем на примере ПЛК Mitsubishi

Антон Дорфман



Обо мне





Антон Дорфман

- Реверс-инженер > 23 лет
- Исследователь прошивок
- Кандидат технических наук

- Ведущий специалист отдела анализа приложений

positive technologies

Спикер

- PHDays, Zeronights, HITBSecConf (Amsterdam), Hackron (Tenerife)

Автор

- CVE в Mitsubishi Electric, Schneider Electric, WAGO, CODESYS
- CPU-модуль NIOS II для IDA Pro (Hex-Rays Plugin Contest)
- Атаки на ПЛК с принтера с модифицированной прошивкой

Чем я занимаюсь



Увлечения

- Прошивки с редкими архитектурами CPU
- Автоматизация задач Reverse Engineering
- Промышленные ПЛК и embedded-устройства

Специализация

- Протоколы и форматы данных
- Уязвимости
- Шеллкоды - импланты в прошивки

Инструментарий

- Декомпилятор Hex-Rays
- Дизассемблер IDA Pro -> idb
- Скрипты на IDAPython
- Сетевой анализатор Wireshark
- Скрипты на Python

Архитектура CPU

- x86/x64
- ARM/ARM64
- PowerPC/PPC64, MIPS/MIPS64
- **Hitachi/Renesas H8/SuperH**
- **NIOS, ???**

В прошивке

- Отладочные символы
- Части исходников в Интернет
- Сообщения об ошибках
- **Текстовые строки**
- **Нет текстовых строк**



Структура доклада



1. Введение
2. Предварительный анализ
3. Исследование
4. Reverse Engineering
5. Результаты
6. Уязвимости
7. Демо

Введение



Что такое ПЛК

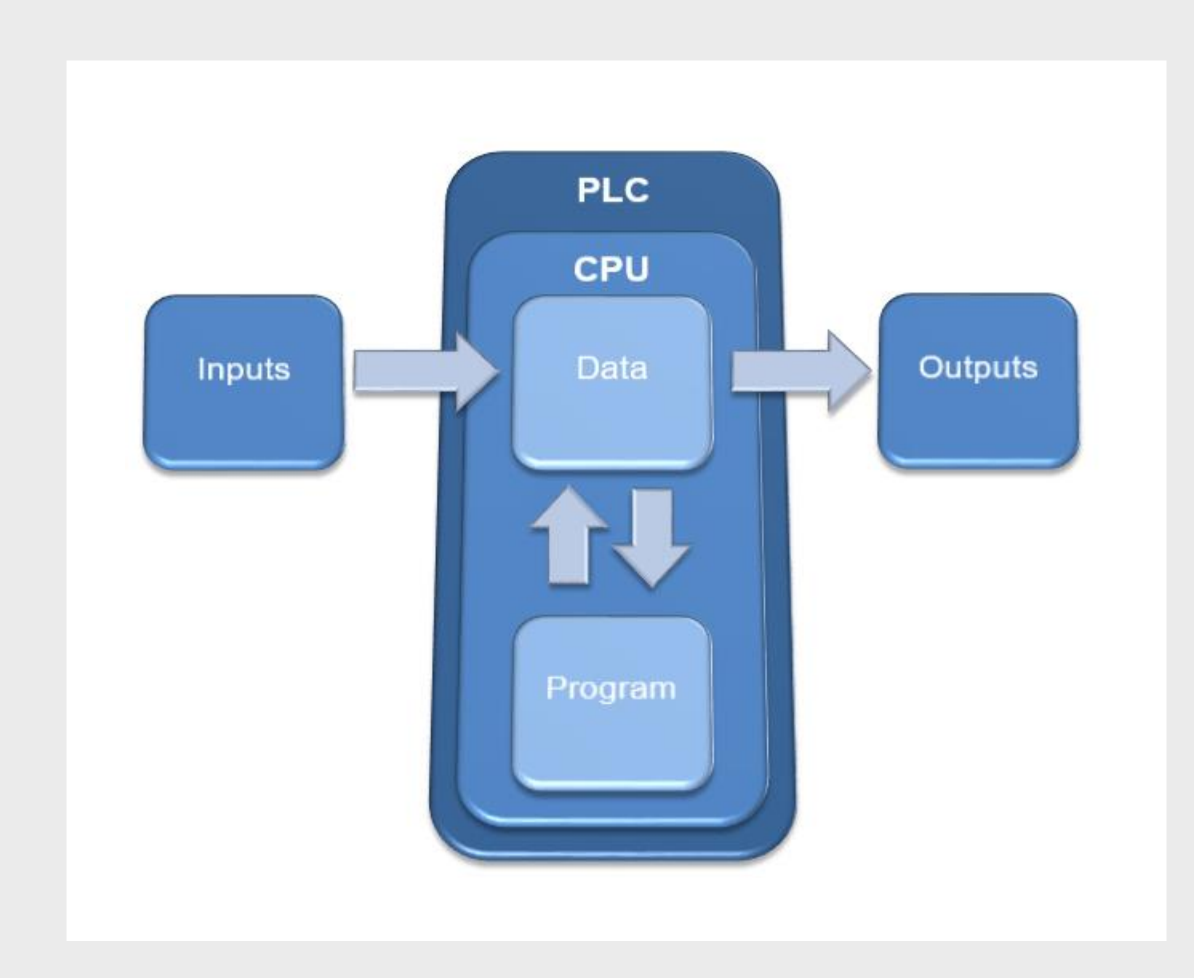
- **Программируемый логический контроллер** (ПЛК, PLC) – это разновидность ЭВМ, для работы в системах реального времени
- **Применение** – автоматизация технологических процессов
- **Основной режим работы** – длительное автономное использование без серьезного обслуживания и без вмешательства в работу

ПЛК в отличие от

- микроконтроллера – самостоятельное устройство, а не отдельная микросхема
- встраиваемой системы – ПЛК отделен от управляемого им оборудования
- компьютера, который управляется оператором – ориентирован на работу с датчиками через входы и исполнительными устройствами через выходы

Промышленные ПЛК





Hardware

- CPU: ARM, PowerPC, MIPS, X86, NIOS и др.
- ROM, RAM, Flash, Network Card, Data Bus

Software

- ОС реального времени, многозадачность
- Файловая система, свои форматы файлов
- Шифрование обновлений
- Парольная защита доступа и др.

Network

- Ethernet, TCP/IP, SNMP, HTTP, FTP и др.
- Modbus, OPC, IEC и др.
- Проприетарные протоколы



Технологическая сеть глазами злоумышленника



Интернет	КСПД (ДМЗ)	Верхний уровень ТС	Средний уровень ТС	Нижний уровень ТС
Внешний сервер	Смежная система (ERP, MES и т.д.); Шлюз	Сервер; АРМ начальника; АРМ оператора; АРМ инженера; Сервер SCADA	ПЛК	Датчики; Исполнительные устройства

А что, если он сможет подключится ?





Какие последствия могут быть?

Правильный ответ на вопрос разный





Влияние на технологический процесс:

- Остановка процесса
- Блокирование запуска
- Подмена управляющих входов и выходов
- Подмена параметров и настроек

Последствия:

- Бракованные изделия
- Авария на производстве
- Остановка предоставления ресурсов
- Техногенная катастрофа

Реальные случаи атак



2010 Stuxnet

Протокол между Simatic S7 и SCADA WinCC

“Нарушил работу почти 1000 центрифуг для обогащения уранового топлива”, “Приостановил ядерную программу Ирана”

2016 Industroyer

IEC 101, IEC 104, IEC 61850, OPC DA

Электрические подстанции

2022 Pipedream

FINS, Modbus CODESYS, OPC UA, некоторые ПЛК Omron , Schneider Electric

Электрические подстанции и производство сжиженного газа

2021-22 Атаки

Водоснабжение: Атака 55 ПЛК Berghof (Израиль)

ТЭК: Colonial Pipeline (США), гидроэлектростанция Гури (Венесуэла), нефтебазы Oiltanking и Mabanaft (Германия), нефтетерминалы SEA-invest (Бельгия) и Evos (Нидерланды)

Металургия: 3 сталелитейных завода (Иран)

Производство: 14 заводов Kojima Industries (Япония), ветряные турбины Nordex (Германия)

Агропромышленность: остановка техпроцессов “Мираторг” (РФ), остановка завода “Тавр”(РФ)

Транспорт: временный паралич ЖД Белорусии, ЖД Польши, ЖД Дании, ЖД Италии

Mitsubishi



- Входит в тройку мировых лидеров
- Выпустила > 17 миллионов ПЛК

MELSEC iQ-R series
MELSEC Q series
MELSEC L series
MELSEC iQ-F series
MELSEC-F
Емкость системы

Medium – Big
Small – Medium
Small

Микроэлектроника
Энергетика
Автотранспорт
Логистика

Оборудование общего назначения (упаковка, пищевая промышленность, литье)

Часто

- Насосные станции
- Канализационно-насосные станции
- Вентиляция в зданиях

Редко

- Вагоноопрокидыватели
- Системы на ТЭЦ
- Шлюзы на водохранилищах

Задачи исследования



- Разобрать протокол и получить его описание
- Научиться общаться в ПЛК с помощью скриптов
- Найти уязвимости в ПЛК

Как вам такой трафик?




```
00000004  57 01 00 00 00 11 11 07  00 00 ff ff 03 00 00 fe   W....... ........
00000014  03 00 00 20 00 1c 0a 16  14 00 00 00 00 00 00 00   ... .... ........
00000024  00 00 00 00 00 00 00 00  00 00 00 00 00 01 21 01   ........ ......!.
00000034  00 00 00 00 01                                     .....
    0000001C  d7 01 00 00 00 11 11 7f  00 00 00 a8 03 00 ff ff   ........ ........
    0000002C  03 00 00 38 00 9c 0a 18  14 00 00 00 00 00 00 00   ...8.... ........
    0000003C  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 01   ........ ........
    0000004C  21 01 00 00 00 46 58 35  55 2d 33 32 4d 52 2f 45   !....FX5 U-32MR/E
    0000005C  53 00 00 00 00 21 4a 00  08 00 00 00 00            S....!J. .....
00000039  57 01 01 00 00 11 11 07  00 00 ff ff 03 00 00 fe   W....... ........
00000049  03 00 00 23 00 1c 0a 16  14 00 00 00 00 00 00 00   ...#.... ........
00000059  00 00 00 00 00 00 00 00  00 00 00 00 00 01 a0 02   ........ ........
00000069  00 00 00 02 89 49 22 d4                            .....I".
    00000069  d7 01 01 00 00 11 11 7f  00 00 00 a8 03 00 ff ff   ........ ........
    00000079  03 00 00 24 00 9c 0a 18  14 00 00 00 00 00 00 00   ...$.... ........
    00000089  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 01   ........ ........
    00000099  a0 02 00 00 00 67 0a 6a  e8                        .....g.j .
```

Предварительный анализ




```
00000004  57 01 00 00 00 11 11 07  00 00 ff ff 03 00 00 fe   W....... ........
00000014  03 00 00 20 00 1c 0a 16  14 00 00 00 00 00 00 00   ... .... ........
00000024  00 00 00 00 00 00 00 00  00 00 00 00 00 01 21 01   ........ ......!.
00000034  00 00 00 00 01                                     .....
    0000001C  d7 01 00 00 00 11 11 7f  00 00 00 a8 03 00 ff ff   ........ ........
    0000002C  03 00 00 38 00 9c 0a 18  14 00 00 00 00 00 00 00   ...8.... ........
    0000003C  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 01   ........ ........
    0000004C  21 01 00 00 00 46 58 35  55 2d 33 32 4d 52 2f 45   !....FX5 U-32MR/E
    0000005C  53 00 00 00 00 21 4a 00  08 00 00 00 00            S....!J. .....
00000039  57 01 01 00 00 11 11 07  00 00 ff ff 03 00 00 fe   W....... ........
00000049  03 00 00 23 00 1c 0a 16  14 00 00 00 00 00 00 00   ...#.... ........
00000059  00 00 00 00 00 00 00 00  00 00 00 00 00 01 a0 02   ........ ........
00000069  00 00 00 02 89 49 22 d4                            ......I".
    00000069  d7 01 01 00 00 11 11 7f  00 00 00 a8 03 00 ff ff   ........ ........
    00000079  03 00 00 24 00 9c 0a 18  14 00 00 00 00 00 00 00   ...$.... ........
    00000089  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 01   ........ ........
    00000099  a0 02 00 00 00 67 0a 6a  e8                        .....g.j .
```

M Protocol



[Request]		Binary 3E	Binary 4E	ASCII 3E	ASCII 4E
Subheader	Fixed value	2 bytes	2 bytes	4bytes	4bytes
	Serial number	N/A	2 bytes	N/A	4bytes
	Free	N/A	2 bytes	N/A	4bytes
Access route	Network No.	1 byte	1 byte	2 bytes	2 bytes
	PC No.	1 byte	1 byte	4bytes	4bytes
	Request destination module I/O No.	2 bytes	2 bytes	2 bytes	2 bytes
	Request destination module station No.	1 byte	1 byte	2 bytes	2 byt
Request data length		2 bytes	2 bytes	4bytes	4byte
Monitoring timer		2 bytes			
Request data	Command	2 bytes	2 bytes	2 bytes	2 byt
	subcommand	2 bytes	2 bytes	2 bytes	2 byt
	Number of word access points				
	Number of double word access points				
	Device number				
	Device code				

Fixed Value

Response data length

End code

[Response]		Binary 3E	Binary 4E	ASCII 3E	ASCII 4E
Subheader	Fixed value	2 bytes	2 bytes	4bytes	4bytes
	Serial number	N/A	2 bytes	N/A	4bytes
	Free	N/A	2 bytes	N/A	4bytes
Access route	Network No.	1 byte	1 byte	2 bytes	2 bytes
	PC No.	1 byte	1 byte	4bytes	4bytes
	Request destination module I/O No.	2 bytes	2 bytes	2 bytes	2 bytes
	Request destination module station No.	1 byte	1 byte	2 bytes	2 bytes
Response data length		2 bytes	2 bytes	4bytes	4bytes
End code		2 bytes	2 bytes	4bytes	4bytes

"The Sum Of All Fears, When ICS SCADA Are Compromised" Selmon Yang, Mars Cheng, TXOne Networks and Trend Micro, HITB+ Cyber Week, Abu Dhabi, UAE: 12-17 October 2019

M Protocol vs PCAP (Read Random)



[Request] Binary 3E		
Subheader	Fixed value	50 00
	Serial number	N/A
	Free	N/A
Access route	Network No.	00
	PC No.	ff
	Request destination module I/O No.	ff 03
	Request destination module station No.	00
Request data length		14 00
Monitoring timer		0a 00
Request data	Command	03 04
	subcommand	00 00
	Number of word access points	02
	Number of double word access points	01
	Device number	00 00 00
	Device code	a8
	Device number	08 00 00
	Device code	a8
	Device number	0b 00 00
	Device code	a8

50 00

00

ff

ff 03

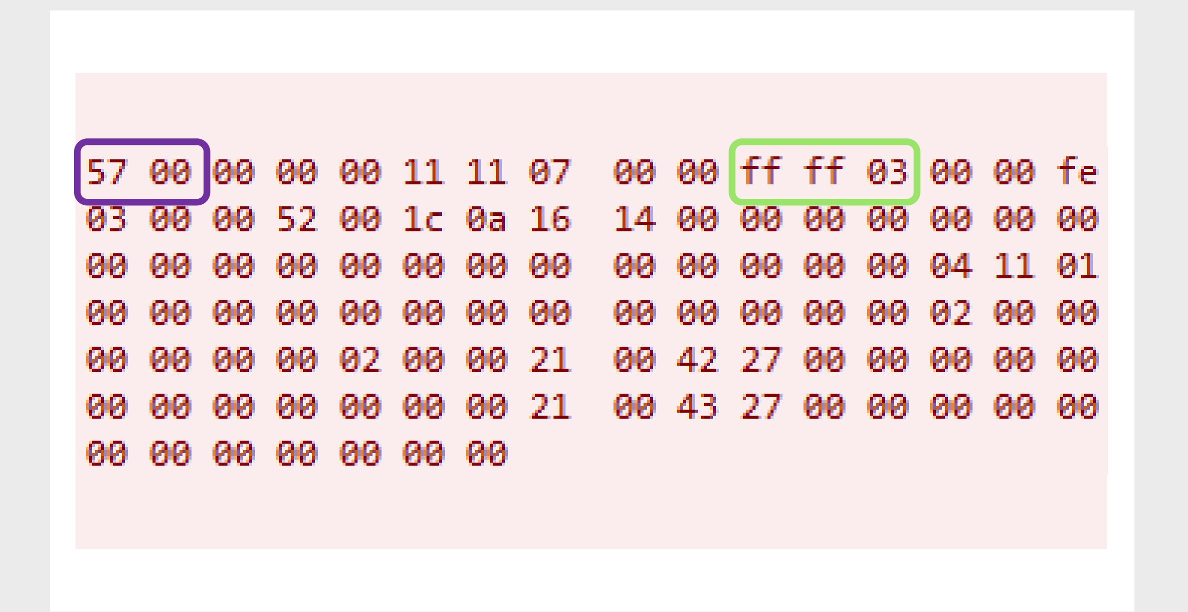
00

03 04

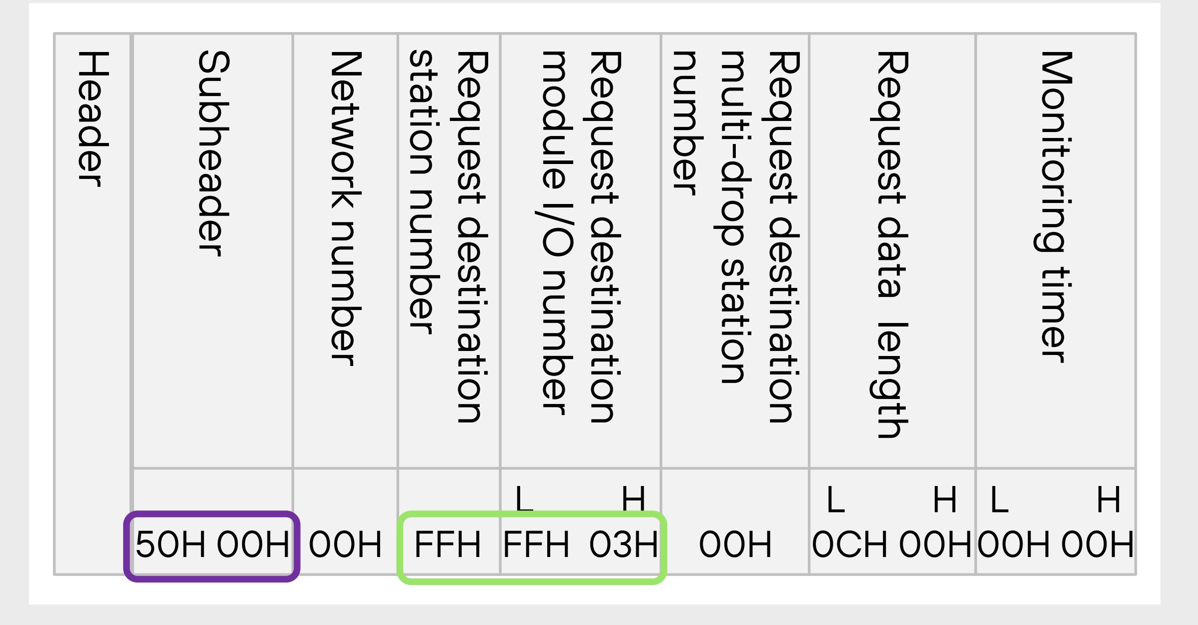
```
57 00 00 00 00 11 11 07  00 00 ff ff 03 00 00 fe
03 00 00 52 00 1c 0a 16  14 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00  00 00 00 00 00 04 11 01
00 00 00 00 00 00 00 00  00 00 00 00 00 02 00 00
00 00 00 00 02 00 00 21  00 42 27 00 00 00 00 00
00 00 00 00 00 00 00 21  00 43 27 00 00 00 00 00
00 00 00 00 00 00 00
```

PCAP vs Manual (Read Random)





```
57 00 00 00 00 11 11 07  00 00 ff ff 03 00 00 fe
03 00 00 52 00 1c 0a 16  14 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00  00 00 00 00 00 04 11 01
00 00 00 00 00 00 00 00  00 00 00 00 00 02 00 00
00 00 00 00 02 00 00 21  00 42 27 00 00 00 00 00
00 00 00 00 00 00 00 21  00 43 27 00 00 00 00 00
00 00 00 00 00 00 00
```



Header	Subheader	Network number	Request destination station number	Request destination module I/O number (L H)	Request destination multi-drop station number	Request data length (L H)	Monitoring timer (L H)
	50H 00H	00H	FFH	FFH 03H	00H	0CH 00H	00H 00H

Device Read Random	0403H

	Sub command	Word access Points	Dword access Points	Word access	
				Device No.	Device code
03H 04H	XX XX	XX	XX	XX XX XX	

M Protocol vs Manual (Read Random)



[Request] Binary 3E		
Subheader	Fixed value	50 00
	Serial number	N/A
	Free	N/A
Access route	Network No.	00
	PC No.	ff
	Request destination module I/O No.	ff 03
	Request destination module station No.	00
Request data length		14 00
Monitoring timer		0a 00
Request data	Command	03 04
	subcommand	00 00
	Number of word access points	02
	Number of double word access points	01
	Device number	00 00 00
	Device code	a8
	Device number	08 00 00
	Device code	a8
	Device number	0b 00 00
	Device code	a8

50 00

00

ff

ff 03

00

03 04

00 00 00	Device Number
a8	Device Code

Header	Subheader	Network number	Request destination station number	Request destination module I/O number		Request destination multi-drop station number	Request data length		Monitoring timer	
				L	H		L	H	L	H
	50H 00H	00H	FFH	FFH	03H	00H	0CH	00H	00H	00H

Device Read Random	0403H

	Sub command	Word access Points	Dword access Points	Word access	
				Device No.	Device code
03H 04H	XX XX	XX	XX	XX XX XX	



Предварительные результаты

```
PORT      STATE         SERVICE
5560/udp  open|filtered unknown
5561/udp  open|filtered unknown
5565/udp  open|filtered unknown
```

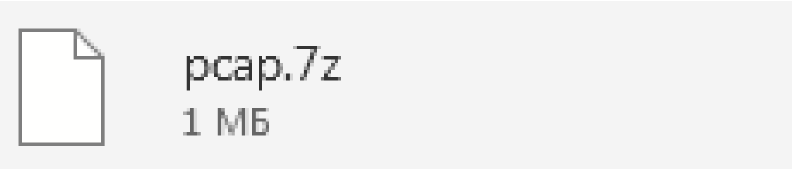
```
PORT     STATE SERVICE
5562/tcp open  unknown
```

MitsuClass.py

1001_Run.py

1002_Stop.py

1003_Pause.py



Показать все: Вложений: 1 (1 МБ)   Скачать

Во первых: ОНО РАБОТАЕТ НА РЕАЛЬНОМ ПЛК !!!!!!!!!!!!!!!!!!!!!!!!!!

АНТОХА – МОЛОДЕЦ!!!!!!!!!!

Прям : старт - стартует, стоп – останавливает, а на паузе – моргает.

Исследование



Проблемы с получением прошивки

- Обновления прошивок свободно скачиваются
- НО! Прошивки зашифрованы
- По косвенным признакам шифрование AES128, проверка целостности - SHA256 и ECDSA256
- Ключи AES и параметры ECDSA в прошивке (до расшифровки) не светятся, и без чтения флеша ничего извлечь не получится

- Выпаяли и сдампили внешнюю флеш-память, прошивки на ней нет
- Прозвонили ножки CPU, подцепились к JTAG, успешно соединились программатором
- CPU вернул, что залочен и требуется “ID Code” для дальнейшего общения
- Не смогли сдампить флеш-память CPU



Правило RTFM, или Учи матчасть!

- **Управление ПЛК**: Run, Stop, Reset, Pause
- **Внутренние устройства (Devices)** – доступны для чтения и записи, по сути регионы памяти ПЛК
- **Функции безопасности**
- **Обновление** – прошивка на SD-карте
- **Файловая система:** создание, открытие, чтение, запись, закрытие и т.д.
- **Настройка параметров ПЛК, загрузка проектов через файловую систему**
- Настройки даты и времени

Device	Type	ASCII	Bin
Input	Bit	X	9Ch
Output		Y	9Dh
Internal relay		M	90h
Data register	Word	D	A8h
Link register		W	B4h

Parameter	☐
System Parameter/CPU Parameter	☐
Module Parameter	☐
Memory Card Parameter	
Remote Password	☐
Program	☐
MAIN	☐

GX Works 3



- Создание программ: Ladder, ST, FBD/LD, SFC
- Настройка параметров: CPU, I/O модулей, проекта
- Чтение из / запись в Device
- Мониторинг и отладка
- Диагностика

Что можем достать

- **Команды** – пункты меню
- **Устройства** – монитор пакетного чтения/записи
- **Параметр настройки** – разница в файлах



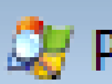
Симулятор

- Обращается к localhost
- Трафик совпадает с ПЛК
- Только по TCP
- Порт вида 55xx, не 5562

Project
RESET RUN
STOP
R04CPU
:Writing data
Simulating
Operation of a programmable controller can be checked in a personal computer without using the actual module.
Project
Virtual programmable controller (GX Simulator3)
GX Simulator3
Tool
1.1 R04CPU
LED
READY
ERROR
P. RUN
USER
SWITCH
RUN
STOP
RESET



Строение симулятора



Process Explorer - Sysinternals:

Command line:

\FSimRun3.exe" --sys 1 --phs 0 --config *34A29-G9044-CPU1 --tcp

GXW3.exe	57860		MITSUBISHI
FSimRun3.exe	61492	GX Simulator 3	MITSUBISHI
FSim3Dlg.exe	61984	Sim3Dlg	MITSUBISHI

-> FX5U.dll ->

FX5U CPU

FX5U-32MT/ES

C:\Windows\system32\cmd.exe

```
C:\RE_FType>FSimRun3.exe --sys 1 --phs 0 --config *34A29-G9044-CPU1 --tcp 5562 -
-reconfig

TOPPERS/JSP Kernel Release 1.4 (patchlevel = 4) for GX Simulator 3 (Nov 23 2016,
 20:23:11)
Copyright (C) 2000-2003 by Embedded and Real-Time Systems Laboratory
                            Toyohashi Univ. of Technology, JAPAN
Copyright (C) 2004-2006 by Embedded and Real-Time Systems Laboratory
            Graduate School of Information Science, Nagoya Univ., JAPAN
```

Брутфорс команд



ПЛК – 83 команды

```
c:\TestPLC\Mitsubishi>BruteCmd.py
-- Connect to Host IP: 10.159.17.12

Good Cmd: 0103
Good Cmd: 0114
Good Cmd: 0121
Good Cmd: 0140
BadParam Cmd: 01A0 EndCode: 4080
BadParam Cmd: 0240 EndCode: 4080
BadParam Cmd: 0410 EndCode: 4031
BadParam Cmd: 0411 EndCode: 4031
BadParam Cmd: 0412 EndCode: 4031
BadParam Cmd: 0413 EndCode: 4030
BadParam Cmd: 0414 EndCode: 4031
```

Симулятор – 54 команды

```
c:\RE_FType>BruteCmd.py
-- Connect to Host IP: 127.0.0.1

Good Cmd: 0103
Good Cmd: 0114
Good Cmd: 0121
Good Cmd: 0140
BadParam Cmd: 0240 EndCode: 4022
BadParam Cmd: 0410 EndCode: 4030
Good Cmd: 0411
Good Cmd: 0412
BadParam Cmd: 0413 EndCode: 4030
Good Cmd: 0414
```

Reverse Engineering



- Нет символов
- Минимум строк

- Документация для похожего протокола
- Коды ошибок из документации
- Результаты нашего исследования
- Знание, как все должно работать
- Скрипты для работы с протоколом
- Результаты брутфорса

Симулятор можно исследовать в отладчике

Документация для похожего протокола



```
type_2:
                call    Type2_CmdHandler
                pop     ecx
                retn
; -----------------------------------------
type_1_other:

                call    Type1_CmdHandler
                pop     ecx
                retn
Type_CmdHandler endp
```

```
case 1u:
  result = Type2_Cmd_04_01(result);
  break;
case 3u:
  result = Type2_Cmd_04_03(result);
  break;
case 6u:
  result = Type2_Cmd_04_06(result);
  break;
```

```
call    sub_71927630
```

xrefs to sub_71927630

Direction	Type	Address	Text
Up	p	Type2_Cmd_04_03+127	call sub_71927630
Up	p	Type1_Cmd_04_11_12+A0	call sub_71927630

Device Read Random	0403H

Коды ошибок из документации




```
cmp     [esp+20h+var_E], eax
jbe     short loc_718FCD24
mov     ecx, 413Ah
mov     [ebx+PACKET_DESCR.EndCode], cx
```

Error code	Error name	Error details and cause
413AH	File related error	The specified file has exceeded the already existing file size.

```
cmp     [esp+20h+FileReadStack.ReadSizeLoc], eax
jbe     short loc_718FCD24
mov     ecx, 413Ah
mov     [ebx+PACKET_DESCR.EndCode], cx
```

Проецирование адресов внутри симулятора




```
movzx   esi, di
mov     ecx, 66184h
movzx   edi, bl
call    GetRealAddr
add     eax, edi
mov     bp, [eax+esi]
or      bp, word ptr [esp+esi+0BCh+a6]
mov     ecx, 66000h
call    GetRealAddr
```

```
movzx   esi, di
mov     ecx, offset Input_After_Start
movzx   edi, bl
call    GetRealAddr
add     eax, edi
mov     bp, [eax+esi]
or      bp, word ptr [esp+esi+0BCh+a6]
mov     ecx, offset Input_Start ; Addr
call    GetRealAddr
```

Скрипты

- Анализ обращений за пределы существующих сегментов
- Группировка смещений – создание сегментов
- Обозначение смещений внутрь новых сегментов



Результаты



MsgHdr					Data Hdr	End Code	NullBlock	Cmd Hdr	Cmd Data
Low Hdr	Flags Hdr	DstRoute Hdr	SrcRoute Hdr	DataSize					

```
00000039  57 00 00 00 00 11 11 07  00 00 ff ff 03 00 00 fe   W....... ........
00000049  03 00 00 52 00 1c 0a 16  14 00 00 00 00 00 00 00   ...R.... ........
00000059  00 00 00 00 00 00 00 00  00 00 00 00 00 04 11 01   ........ ........
00000069  00 00 00 00 00 00 00 00  00 00 00 00 00 02 00 00   ........ ........
00000079  00 00 00 00 02 00 00 21  00 42 27 00 00 00 00 00   .......! .B'.....
00000089  00 00 00 00 00 00 00 21  00 43 27 00 00 00 00 00   .......! .C'.....
00000099  00 00 00 00 00 00 00                               .......
    00000069  d7 00 00 00 00 11 11 7f  00 00 00 a8 03 00 ff ff   ........ ........
    00000079  03 00 00 26 00 9c 0a 18  14 00 00 00 00 00 00 00   ...&.... ........
    00000089  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 04   ........ ........
    00000099  11 01 00 00 00 00 00 0c  11 9f 0a                  ........ ...
```

Устройства и команды



Dev Idx	Name	ASCII	Bin
01h	Internal relay	M	90h
02h	Special relay	SM	91h
03h	Latch relay	L	92h
04h	Annunciator	F	93h
08h	Step relay	S	98h
10h	Input	X	9Ch
11h	Output	Y	9Dh
20h	Data register	D	A8h
27h	File register	R	AFh
30h	Link register	W	B4h
40h	Timer Contact	TS	C1h
60h	Index register	Z	CCh

New	Cmd Name	Man
0121	Model Name	0101
0410	Batch Read	0401
0411	Random Read	0403
1001	Remote RUN	1001
1002	Remote STOP	1002
100A	Remote RESET	1006
1410	Batch Write	1401
1411	Random Write	1402
1867	Open File	1827
1868	Read File	1828
1869	Write File	1829
186A	Close File	182A

Демо Knight Rider K.I.T.T.





Взаимодействие с вендором



15.12.21	Отправили отчет в Mitsubishi
21.12.21	Ответ – разослали по департаментам
14.01.22	Подтверждение проверки 8 уязвимостей в ПЛК, релиз Advisory в феврале 2022
21.01.22	Ответ от департамента GX Works 3, что релиз Advisory в ноябре 2022
18.02.22	Запрос по сдвигу сроков публикации уязвимостей в ПЛК
31.03.22	Релиз информации о 6 уязвимостях в ПЛК: CVE-2022-25155, CVE-2022-25156, CVE-2022-25157, CVE-2022-25158, CVE-2022-25159, CVE-2022-25160
17.05.22	Релиз информации о 2 уязвимостях в ПЛК: CVE-2022-25161, CVE-2022-25162
31.05.22	Обновили информацию по всем восьми уязвимостям в ПЛК
??.11.22	Релиз информации о 7 уязвимостях в GX Works 3

Advisory
https://www.mitsubishielectric.com/en/psirt/vulnerability/pdf/2022-004_en.pdf
https://www.mitsubishielectric.com/en/psirt/vulnerability/pdf/2021-031_en.pdf

Уязвимости



CVE	Description	CVSS
CVE-2022-25155	Use of Password Hash Instead of Password for Authentication(CWE-836)	5.9
CVE-2022-25156	Use of Weak Hash(CWE-328)	5.9
CVE-2022-25157	Use of Password Hash Instead of Password for Authentication(CWE-836)	7.4
CVE-2022-25158	Cleartext Storage of Sensitive Information(CWE-312)	7.4
CVE-2022-25159	Authentication Bypass by Capture-replay(CWE-294)	5.9
CVE-2022-25160	Cleartext Storage of Sensitive Information(CWE-312)	6.8
CVE-2022-25161	Improper Input Validation(CWE-20)	8.6
CVE-2022-25162	Improper Input Validation(CWE-20)	5.3

If these vulnerabilities are exploited by a malicious attacker, an unauthenticated attacker may be able to login to the products or the information in the products may be disclosed or tampered with.
MELSEC Series: iQ-F, iQ-R, Q, L.

These vulnerabilities could allow a malicious attacker to cause a DoS condition for a product's program execution or communication by sending specially crafted packets. For CVE-2022-25161, a system reset of the product is required for recovery.
MELSEC iQ-F series: FX5U(C), FX5UJ

Уязвимость CVE-2022-25161



DevOff_To_RealAddr: RealAddr = DevStartAddr + DevOff * UnitSize (UnitSize=2)

DevStartAddr = 0x66000

DevOff = 0xFFFCD000

RealAddr = 0x66000 + DevOff * 2

RealAddr = 0x66000 + 0xFFFCD000 * 2 = 0



DevOff проверяется на Max – сравнивается с размером устройства DevSize

Если RealAddr = 0, тогда проверки DevOff на Max не происходит

```
v9 = DevOff_To_RealAddr(&Dev_Off_To_Addr_RetVal, &RetRealAddr, RdWrAddr, v6);
v11 = RndRdWrAddrLoc.DevIdx;
v12 = v9;
DevStrucIdx = v9;
if ( !RetRealAddr )
  goto RealAddr_is_Null;
```

Демо PoC CVE-2022-25161 на макете нефть



Нефтеперекачивающая станция

- Магистральные насосные агрегаты
- Запорные и регулирующие задвижки
- ПЛК управляет насосами и задвижками
- Состояние и параметры техпроцесса на экране SCADA



Уязвимость CVE-2022-25162




```
00000000: 00 01 58 00 04 00 02 01|08 00 03 00 00 00 10 02  | ..X.............
00000010: 44 00 04 00 00 00 00 00|00 00 00 00 00 00 00 00  | D...............
00000020: 00 00 00 00 00 00 00 00|00 00 00 00 00 00 00 00  | ................
00000030: 00 00 00 00 00 00 00 00|00 00 00 00 00 00 00 00  | ................
00000040: 00 00 00 00 00 00 00 00|00 00 00 00 00 00 00 00  | ................
00000050: 00 00 00 00 FF FF FF FF|3B 00 00 00 8B 88 32 C1  | ....¤¤¤¤;...ЛИ2S
00000060: C9 D7 47 10 C0 4F 21 52|72 02 E2 C6 EE B8 5E 90  | …„G.jO!Rr.в△oЄ^P
00000070: 1F E9 39 67 30 77 2D D6|63 72 FD 55 00 00 00 00  | .й9g0w-÷crэU....
00000080: 00 00 00 00 00 00 00 00|00 00 00 00 00 00 00 00  | ................
00000090: 00 00 00 00 00 00 00 00|00 00 00 00 01 00 09 00  | ................
000000A0: 00 00 00 00 FF 00 00 00|00 00 00 00 00 00 00 00  | ....¤...........
000000B0: 00 00 24 00 00 00 00 00|00 00 00 00 00 00 00 00  | ..$.............
000000C0: 00 00 00 00 00 00 00 00|00 00 00 00 00 00 00 00  | ................
000000D0: FF FF 00 00 00 00 D0 2F|A1 03 02 10              | ¤¤....-/°...|
```

Размер для контрольной суммы: FileBodySize = FileSize - HeaderSize

```
00000000: 48 41 43 4B 45 52      |                         | HACKER
```

FileBodySize = 6 - 0x4B43 = 0xFFFFB4C3

Демо PoC CVE-2022-25162 на макете вода



Водозаборная станция

- Установки для обработки воды
- Резервуары чистой воды
- Насосы для перекачки из водоема
- ПЛК управляет насосами
- Состояние и параметры техпроцесса на экране SCADA



Сравнение PoC



CVE-2022-25161 CVSS:3.1: **8.6**

Действие на ПЛК:

- ПЛК в ошибке
- Программа не работает
- Выходы гаснут
- Нет связи по всем портам
- Не пингуется

CVE-2022-25162 CVSS:3.1: **5.3**

Действие на ПЛК:

- ПЛК работает
- Программа работает
- Выходы не гаснут
- Нет связи по порту соединения
- Пингуется

Добавка к PoC

- Вышибаем СКАДА, если он подключен к порту 5560
- Применяем DoS по очереди для каждого порта
- Нет связи по основным портам



Итоги исследования

- Разобрать протокол и получить его описание 
- Научиться общаться в ПЛК с помощью скриптов 
- Найти уязвимости в ПЛК 

Благодарю за внимание!

Вопросы?



dorfmananton@gmail.com

@AntonDorfman



Оценить доклад

